

# Maîtrisez votre Cyberscore : les étapes clés pour une conformité totale

---

## Inventaire et périmètre technique

- Réaliser un inventaire exhaustif de tous les actifs numériques : noms de domaine, sous-domaines et applications web.
- Délimiter précisément le périmètre de l'audit pour garantir une couverture complète des services exposés.

## Sécurisation des flux et des accès

- Activer exclusivement le protocole TLS 1.3 et désactiver les versions obsolètes (TLS 1.0, 1.1) ainsi que les suites de chiffrement faibles.
- Utiliser des certificats SSL/TLS valides avec une clé RSA d'au moins 2048 bits.
- Implémenter l'authentification multifacteur (MFA) pour tous les accès au back-office, aux interfaces d'administration et aux comptes à privilèges.
- Configurer les en-têtes de sécurité HTTP (Content-Security-Policy, X-Content-Type-Options, Strict-Transport-Security) pour prévenir les attaques XSS et injections.

## Conformité RGPD et gestion des données

- Publier une Politique de Confidentialité conforme au RGPD, incluant les coordonnées du DPO et le détail des durées de conservation des données.
- Mettre en œuvre un mécanisme de gestion des cookies respectant les lignes directrices de la CNIL (consentement préalable et refus aussi simple que l'acceptation).

## Maintenance, indexation et résilience

- Auditer les vulnérabilités des bibliothèques tierces (JS, CMS) via des outils comme 'npm audit' ou 'OWASP Dependency-Check'.
- Protéger les zones d'administration et les données sensibles contre l'indexation via le fichier 'robots.txt' et les balises meta 'noindex'.
- Automatiser les sauvegardes chiffrées et déportées de l'intégralité du site et de la base de données, avec des tests de restauration réguliers.